

(43) Date of publication of application: 11.03.88

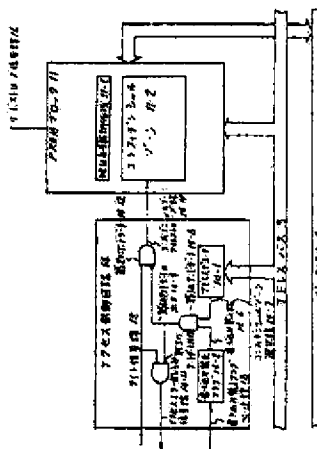
(22) Date of filing: 27.08.86

(72) Inventor: FUJIMURA YOSHIHIDE  
OKAMOTO WATARU

(57) Abstract:

**CONSTITUTION:** An access control circuit 14 is composed of an address decoder 14-1, a writing prohibiting flag 14-2 and three two-input AND gates. When the address decoder 14-1 decodes address data on an address bus 3 and the area of a confidential zone 11-2 is selected, a confidential zone selecting line 14-7 is made into a high level. The writing prohibiting flag 14-2 is the flag to prohibit the writing to the confidential zone 11-2, is set by the exclusive-sue instruction of the processor and once setting is executed, is the semi-fixed flag which cannot be reset.

COPYRIGHT: (C)1988, JPO&Japio



⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭63-56749

⑬ Int.Cl.<sup>4</sup>

G 06 F 12/14  
15/06

識別記号

3 1 0  
3 2 0

庁内整理番号

F-7737-5B  
A-7343-5B

⑭ 公開 昭和63年(1988)3月11日

審査請求 未請求 発明の数 1 (全9頁)

⑮ 発明の名称 シングルチップマイクロコンピュータ

⑯ 特 願 昭61-202231

⑰ 出 願 昭61(1986)8月27日

⑱ 発 明 者 藤 村 善 英 東京都港区芝5丁目33番1号 日本電気株式会社内

⑲ 発 明 者 岡 本 渉 東京都港区芝5丁目33番1号 日本電気株式会社内

⑳ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号

㉑ 代 理 人 弁理士 内 原 晋

明 細 書

1. 発明の名称

シングルチップマイクロコンピュータ

2. 特許請求範囲

単一半導体基盤上に書き込み可能なROM及びコンピュータ機能を集積したシングルチップマイクロコンピュータにおいて、半固定の書き込み禁止フラグ及び前記ROMの特定領域を指定するアドレスデコード回路とを含むアクセス制御回路を備え、前記ROMの特定領域に対して前記アクセス制御回路を用いて書き込みを禁止することを特徴とするシングルチップマイクロコンピュータ。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、単一半導体基盤上にメモリ機能及びコンピュータ機能を集積したシングルチップマイクロコンピュータに関し、とくにプログラム可能

なメモリ(PROM)を内蔵したシングルチップマイクロコンピュータに関する。

(従来の技術)

近年はLSI製造技術の進歩により、シングルチップマイクロコンピュータの分野においても高集積化が進み、単位機能当たりのコストの低下も著しくなっている。

従来、銀行などの金融機関においては磁気カードが主に使用されてきたが、磁気カードは記憶容量が少なく、またセキュリティの面で問題があり、最近では不正使用、偽造など多くの犯罪が頻発し、大きな社会問題となっている。そこでこの磁気カードに代るものとして、シングルチップマイコンを搭載したICカードが登場し、国内外において実用化に向けて大規模な実験が進んでいる。前記ICカードは磁気カードに比べ、記憶容量も数段大きく、またカード内にコンピュータ機能を内蔵しているのでセキュリティの面でも格段の信頼度がある。

一般にシングルチップマイコンを搭載したIC

カードにおいては、データメモリの大部分にUV-EPROM(ultra-Violet Erasable Programmable ROM)またはEEPROM(Electrical Erasable Programmable ROM)を使用しており(以後UVEEPROM, EEPROMを総じてPROMと称する)、そのデータメモリをいくつかの領域に分割しそのアクセスを管理している。

銀行などの金融機関においてキャッシュカード、クレジットカードとしてICカードを使用する場合、この分割されたデータメモリの一部をコンフィデンシャル・ゾーン(Confidential Zone)と呼び、銀行の支店番号、口座番号など機密性の高いデータを格納するのに使用している。このコンフィデンシャル・ゾーンはICカードの不正使用、偽造を防止する上で最も重要な部分であって、従来ソフトウェアにより前記領域に対するアクセスを管理し、通常は一層秘匿データを書込んだら再書き込みは許可せず、特別な場合だけ前記領域に対しアクセスできるようにしている。

以下、データメモリ中にコンフィデンシャル・

結果をデータバス4へ出力する。RAM10は汎用レジスタ及び様々な処理データ格納用として用いられる読み出し、書き込みが可能なメモリで、アドレスバス3でアドレス指定される格納データをデータバス4へ出力するか、データバス4上のデータをアドレスバス3で指定されるアドレスに格納する。RAM10内には、演算の中心となる汎用レジスタ群10-1、カードユーザーが端末より入力したデータをポート12を介して格納する入力データ格納領域10-2、コンフィデンシャル・ゾーン内のデータリードの許可を示す読み出し許可フラグ10-3を有している。

PROM11はデータメモリとしてUVEEPROMまたはEEPROMを内蔵しており、データメモリ内にはカードの暗証番号格納領域11-1、コンフィデンシャル・ゾーン11-2、コンフィデンシャル・ゾーン内に対する書き込みを禁止する書き込み禁止フラグ11-3を有しており、ライト信号線15のハイレベルの信号により、アドレスバス3上のアドレスに対しデータバス4上のデータを

ゾーンを有した従来のシングルチップマイクロコンピュータの例について第5図のマイクロコンピュータのブロック図、第6図のフローチャートを用いて説明する。

まず構成要素の説明を行なう。

第5図においてプログラムカウンタ1は命令コードの格納アドレスを指すポインタである。ROM(Read Only Memory)2はユーザプログラム格納に用いる読み出し専用メモリである。アドレスバス3はアドレスデータを転送するバスである。データバス4は中央処理装置(以下CPUと呼ぶ)の処理データを転送するバスである。命令レジスタ5はROM2から読み出した命令コードを格納するレジスタである。命令デコード6は命令レジスタ5に格納された命令コードで指定されたCPU動作を制御する装置である。テンポラリレジスタ7及び8は算術論理演算ユニット6への入力データを一時保持するためのレジスタである。算術論理演算ユニット9はテンポラリレジスタ7, 8に格納されたデータに対し算術論理演算を行ない、

書き込み、リードストロブ信号線16のハイレベルの信号によりアドレスバス3上のアドレスデータで指定されるデータをデータバス4上に出力する。ポート12は、チップ外部との通信を行なうためのポートで、データバス4のデータを外部に出力し、外部からのデータを入力する機能を持つ。プログラムカウンタ1、命令レジスタ5、命令デコード6、テンポラリレジスタ7及び8、汎用レジスタ群10-1、算術論理演算ユニット9からなるブロックは中央処理装置(CPU)を構成している。割込み制御回路13はポート12などの周辺ハードウェアから発生する割込み信号の受け付け、制御を行ない、CPUに割込み処理を実行させる。

上記構成要素を用いて動作説明を行なう。

PROM11内にコンフィデンシャル・ゾーンを有したシングルチップマイクロコンピュータにおいては、プログラムカウンタ1で指定されるアドレスの命令コードをROM2から読み出し、データバス4を介して命令レジスタ5に格納する。命令

レジスタ5に格納された命令コードは命令デコーダ6へ入力され、プログラマブル・ロジック・アレイ (PLA) などのハードウェアによってデコードされて命令機能が実行される。

例えば汎用レジスタ間の二項演算の場合、汎用レジスタ10-1の内容をRAM10から読み出し、テンポラリレジスタ7及び8に格納する。次に算術論理演算ユニット9を動作させ、演算結果をデータバス4を介してデスティネーションが汎用レジスタの場合RAM10内の汎用レジスタ群10-1の対応したレジスタに書き込む。

次に第6図のフローチャートを用いてPROM11内のコンフィデンシャル・ゾーン11-2へのアクセス方法について説明する。

まず最初にユーザーが外部装置よりキー入力したデータ(暗証番号)をポート12を介してRAM10内のキー入力データ格納領域10-2に格納する。次にROM2に格納されているプログラムにより、キー入力データ格納領域10-2に格納されているキー入力された暗証番号とあらかじめ定

義されていてPROM11内に設定されている暗証番号格納領域11-1の値との比較を行なう。比較した結果、一致した場合は、更に乱数などを発生させてキー入力されたデータに算術論理演算ユニット9で演算処理を施し、同様の演算をオンラインコンピュータで実行後、結果をポート12を介して受け取り、前記演算結果と同一の場合のみ正当なカードアクセスであることを確認する。

前記確認の結果、正当なカードアクセスと判定した場合はRAM10内の読み出し許可フラグ10-3を"1"にし、PROM11内のコンフィデンシャル・ゾーン11-2内のデータ読み出しを許可する。不一致の場合は読み出し許可フラグ10-3は"0"とし、コンフィデンシャル・ゾーン10-3内のデータ読み出しを許可しないと共に、以後のカードアクセスを禁止する。

次に、ROM2に格納されているプログラムにおいてコンフィデンシャル・ゾーン11-2へのアクセス命令が実行された場合はコンフィデンシャル・ゾーンアクセス判定ルーチン(ROM2内のプ

ログラム)に分岐し、以下の処理を行なう(第6図参照)。

① コンフィデンシャル・ゾーンアクセスルーチンでは、最初に当該命令がデータライト命令かデータリード命令かを判別する。

② ①の結果データライト命令と判定すると、書き込み禁止フラグ11-3の値をチェックし、

"0"の場合は書き込みが許可されたとしてアドレスデータ、書き込みデータを各々アドレスバス3、データバス4に出力後、ライト信号線15をハイレベルにしてコンフィデンシャル・ゾーンへの書き込み動作をPROM11に行なわせる。

そして以後コンフィデンシャル・ゾーンへの書き込みを禁止したい場合には書き込み禁止フラグ11-3を"1"にする。また、書き込み禁止フラグ11-3が"1"の場合は書き込み禁止であるので書き込み動作は行なわず、アクセスエラールーチンを実行する。①の結果データリード命令と判別すると、RAM10内の読み出し許可フラグ10-3の値をチェックし、"1"の場合はコ

ンフィデンシャル・ゾーン内のデータ読み出しが許可されたとしてアドレスバス3にアドレスデータを出力後、リードストロブ線16をハイレベルとし、コンフィデンシャル・ゾーン11-2よりデータをデータバス4上に読み出す。また読み出し許可フラグ10-3が"0"の場合は読み出し動作は行なわず、アクセスエラールーチンを実行する。

③ アクセスエラー処理ルーチンではアクセスエラーの回数の計数などの処理を行ない、その値によりカードを使用不能とするような処理を行なう。

よって最初のカード使用時に、必要なデータをコンフィデンシャル・ゾーン11-2にプロセッサの命令により書き込んでおいて書き込み禁止フラグ11-3をセットし、以後のコンフィデンシャル・ゾーン11-2へのデータ書き込みを禁止しておけば、前記のコンフィデンシャル・ゾーンアクセス判定ルーチンを用いることにより、次回からのカード使用時にはコンフィデ

シャル・ゾーンへの再書き込みは禁止される。

以上述べたように従来のシングルチップマイクロコンピュータにおいては、秘匿データを格納するコンフィデンシャル・ゾーンに対するアクセス管理をすべてユーザーのソフトウェアにより行なっている。このようなマイクロコンピュータをカードに搭載した場合、外部からの通信手段などによる不当なアクセスまたは内蔵ROMパターンの解読により、上記コンフィデンシャル・ゾーンへ不当なデータが書き込まれることが考えられる。またデータメモリとして紫外線消去型読み出し専用メモリ(UVEPROM)が使用されている時は、ROMセルに常に電圧を印加している場合もあるので、プログラムが暴走した時、書き込み禁止フラグのデータが失われたり、コンフィデンシャル・ゾーンに対し不当な書き込みが行なわれ、その結果カードが使用不可能となる危険性がある。さらにデータメモリに電気消去型読み出し専用メモリ(EEPROM)が使用されている場合には、書き込み命令が実行される

とPROM 内部で自動的に書き込み用の電圧が生成されるので、前記UVPROMの場合と同様、コンフィデンシャル・ゾーンに対し、不当な書き込みが行なわれる可能性がある。

(発明が解決しようとする問題点)

上述したように、従来のデータメモリにおける書き込み禁止の領域であるコンフィデンシャル・ゾーンへのアクセスをソフトウェアにより管理しているシングルチップマイクロコンピュータにおいては、秘匿データを格納しているコンフィデンシャル・ゾーンへのアクセス管理をすべてソフトウェアによって行なっているため、そのソフトウェアが何らかの方法で解読されてしまい、不正なアクセスが行なわれてコンフィデンシャル・ゾーン内のデータが失われたり、また故意にデータが書き換えられる危険性が生じる。さらに前記ソフトウェアが暴走した場合、同様にコンフィデンシャル・ゾーン中の秘匿データが書き換えられる危険性があり、ソフトウェアのみによるメモリ管理はフェイル・セーフの面において不完全であるとい

う欠点があった。

(問題点を解決するための手段)

本発明におけるシングルチップマイクロコンピュータは単一半導体基盤上に書き込み可能なROM(Programmable Read Only Memory、以下PROMと称する)及びコンピュータ機能を集積したシングルチップマイクロコンピュータにおいて、半固定の書き込み禁止フラグ及び前記PROM内の特定領域を指定するアドレスコード回路とを含むアクセス制御回路を備え、前記特定領域に対しては前記アクセス制御回路によりその書き込みを禁止することを特徴とする。さらに、前記アクセス制御回路はさらに半固定のアドレスレジスタ及び前記アドレスレジスタの内容とアドレスデータの内容とを比較する比較器とを有し、前記特定領域の指定をフレキシブルに行なえるようにしたことを特徴とする。

(実施例-1)

次に本発明に係わるシングルチップマイクロコンピュータの第1の実施例について第1図、第2

図を用いて説明する。

第1図は本発明に係わる第1の実施例のシングルチップマイクロコンピュータのブロック図である。第2図は第1図におけるアクセス制御回路14の詳細図である。

まず構成要素の説明を行なう。

本発明に係わる第1の実施例のシングルチップマイクロコンピュータにおいては、PROM11と本実施例で新たに追加したアクセス制御回路14以外の構成要素は、第5図に示す従来例と相違がないので、以下PROM11とアクセス制御回路14について構成及び動作を第2図を用いて説明する。

第2図に示すPROM11はUVEPROMまたはEEPROMで、その中には従来例と同様、暗証番号格納領域11-1、コンフィデンシャル・ゾーン11-2を有している。またPROM11はアクセス判定回路14からのコンフィデンシャル・ゾーンライトストロブ信号線14-10を受け取るとアドレスバス3上のアドレスデータで指定されるアドレスにデータバス4上のデータを格納する。

アクセス制御回路14はアドレスデコーダ14-1、書き込み禁止フラグ14-2、及び3個の2入力アンドゲートから構成されるブロックである。

アドレスデコーダ14-1はアドレスバス3上のアドレスデータをデコードし、コンフィデンシャル・ゾーン11-2の領域が選択された場合に、コンフィデンシャル・ゾーン選択線14-7をハイレベルにする。

書き込み禁止フラグ14-2は、コンフィデンシャル・ゾーン11-2への書き込みを禁止するためのフラグで、プロセッサの専用命令でセットし、一旦セットするとリセット不可能な半固定フラグである。第4図に書き込み禁止フラグ14-2の回路構成を示す。書き込み禁止フラグ14-2は高抵抗の抵抗20、抵抗20に比べ十分抵抗値の小さいヒューズ抵抗21、及び書き込み禁止フラグセット線18をセットすることにより、ヒューズ抵抗21を切断することに十分な電流駆動能力のあるnチャネルトランジスタ19より構成され、ヒューズ抵抗21が切断されていない時は書き込み禁止線14

-6からはロウレベルの電圧が出力される。そして書き込み禁止フラグセット線18をプロセッサの専用命令でアクティブにし、nチャネルトランジスタ19をONしてヒューズ抵抗21に電流を流してヒューズ抵抗を切断することにより、以後の書き込み禁止線14-6の出力はハイレベルとなる。

書き込み禁止フラグ14-2の出力である書き込み禁止線14-6とコンフィデンシャル・ゾーン選択線14-7は第1のアンドゲート14-8に入力され、前記アンドゲートの出力14-9は第2のアンドゲート14-12に入力される。

第1のアンドゲートの出力14-9とライト信号線15は第2のアンドゲート14-12に入力され、第1のアンドゲートの出力14-9がロウレベルで、ライト信号線15がハイレベルの時、コンフィデンシャル・ゾーンライトストロブ信号線14-10がハイレベルとなる。

第1のアンドゲートの出力14-9とライト信号線15は第3のアンドゲート14-13に入力され、第1のアンドゲートの出力14-9がハイ

レベル(書き込み禁止中にコンフィデンシャル・ゾーンが選択された時)で、ライト信号15が入力されると、コンフィデンシャル・ゾーンライトストロブ信号線14-10はロウレベルのまま、アクセスエラー割込み信号線14-11よりアクセスエラー割込み信号を割込み処理制御回路13に対し発生する。

上記構成要素を用いて、コンフィデンシャル・ゾーンアクセスの動作説明を行なう。

まず最初にコンフィデンシャル・ゾーン11-2に、カード使用時に必要な最重要秘匿データをプロセッサの命令によりプログラムする。この書き込み動作は、アドレスバス3上のアドレスデータをPROM11内のアドレスデコード部がデコードし、ライト信号線13をハイレベルにすることにより、データバス4上のデータを書込むことにより行なわれる。この時は書き込み禁止フラグ14-2はセットされていないので、第1のアンドゲート14-8の出力14-9は常にロウレベルであり、コンフィデンシャル・ゾーン11-2を含めPROM

メモリ全体に自由にデータを書込むことができる。

次に、以上の動作に必要なデータをコンフィデンシャル・ゾーン11-2に書き込んだら、以後のコンフィデンシャル・ゾーン11-2への書き込みを不可能にするため、プロセッサの専用命令により書き込み禁止フラグセット線18をアクティブにし、書き込み禁止フラグ14-2をセットする。書き込み禁止フラグ14-2は一旦セットされるとリセットできない半固定フラグであるので、以後書き込み禁止線14-6は常にハイレベルとなる。よって以後アドレスデコーダ14-1によりコンフィデンシャル・ゾーンが選択されてコンフィデンシャル・ゾーン選択線14-7がハイレベルとなると、第1のアンドゲートの出力14-9はハイレベルとなり、ライト信号線15がハイレベルであっても第2のアンドゲート14-12の出力であるコンフィデンシャル・ゾーンライトストロブ線14-10はロウレベルとなるので、以後はコンフィデンシャル・ゾーン11-2への書き込みは全く不可能となる。また、もしコンフィデンシ

ャル・ゾーン 11-2 へのデータ書き込み禁止中にデータを書き込む動作を行なえば、第 3 のアンドゲート 14-13 によりアクセスエラー割込み信号線 14-11 より、ノンマスカブルな割込み信号を発生し、プロセッサにアクセスエラーの割込み処理を実行させる。

従って本第 1 の実施例においては、半固定の書き込み禁止フラグなどの簡単なハードウェアを付加することにより、コンフィデンシャル・ゾーン内のデータに対する不当な書き換えや、プログラムの暴走によるコンフィデンシャル・ゾーン内のデータの消失を防ぐことができ、フェール・セーフが完全となる。

以上が本発明の第 1 の実施例におけるコンフィデンシャル・ゾーンへのデータ書き込み動作であるが、コンフィデンシャル・ゾーン内のデータ読み出し動作については従来例と同様に行ない、不正なアクセスに対する対処はソフトウェア処理により行なう。

スタで、上位 7 ビットにより PROM 領域のコンフィデンシャル・ゾーン 11-2 の上位アドレスを記憶し、最下位ビットは書き込み禁止フラグ 14-2 となっている。アドレスレジスタ 14-21 の各ビットは前記第 1 の実施例における書き込み禁止フラグと同様な構成となっており、一度データを書き込んだら書き換え不可能な半固定のレジスタである。またこのレジスタはメモリ上の特別な空間に I/O マップされている。

比較器 14-20 はアドレスバス 3 上のアドレスデータの上位 7 ビットとアドレスレジスタ 14-21 に格納されている 7 ビットのアドレスデータを比較し、一致したらコンフィデンシャル・ゾーン選択線 14-7 をハイレベルにする。

上記構成要素を用いて、コンフィデンシャル・ゾーンアクセスの際の動作説明を行なう。

まず最初に第 1 の従来例と同様にコンフィデンシャル・ゾーン 11-2 にカード使用時に必要な秘密データなどをプロセッサの命令により格納する。この時は書き込み禁止フラグ 14-2 はセット

#### [ 実施例 - 2 ]

次に本発明に係わるシングルチップマイクロコンピュータの第 2 の実施例について、第 1 図、第 3 図を用いて説明する。

第 1 図は本発明における第 2 のシングルチップマイクロコンピュータのブロック図である。この第 1 図のブロック図は第 1 の実施例におけるブロック図と同一のものである。第 3 図は第 1 図におけるアクセス制御回路 14 の詳細図である。

まず構成要素の説明を行なう。

本発明に係わる第 2 の実施例のシングルチップマイクロコンピュータにおいては、アクセス制御回路 14 以外の構成要素は第 1 の実施例のものと相違がないので、以下アクセス制御回路 14 のみについて第 3 図を用いて説明する。

第 3 図に示すアクセス制御回路 14 はアドレスレジスタ 14-21、比較器 14-20、書き込み禁止フラグ 14-2、及び 3 個のアンドゲートを有している。

アドレスレジスタ 14-21 は 8 ビットのレジ

スタで、上位 7 ビットにより PROM 領域のコンフィデンシャル・ゾーン 11-2 の上位アドレスを記憶し、最下位ビットは書き込み禁止フラグ 14-2 となっている。アドレスレジスタ 14-21 の各ビットは前記第 1 の実施例における書き込み禁止フラグと同様な構成となっており、一度データを書き込んだら書き換え不可能な半固定のレジスタである。またこのレジスタはメモリ上の特別な空間に I/O マップされている。

比較器 14-20 はアドレスバス 3 上のアドレスデータの上位 7 ビットとアドレスレジスタ 14-21 に格納されている 7 ビットのアドレスデータを比較し、一致したらコンフィデンシャル・ゾーン選択線 14-7 をハイレベルにする。

次に以上の動作で必要なデータをコンフィデンシャル・ゾーン 11-2 に書き込んだら、アドレスレジスタ 14-21 にコンフィデンシャル・ゾーンを指定するアドレス上位の 7 ビットデータと、書き込み禁止フラグ 14-2 である最下位ビットに 1 を格納する。そして書き込み禁止フラグ 14-2 をセットする。本第 2 の実施例におけるアドレスレジスタ 14-21 は 7 ビットのアドレスデータを格納する構成になっているので、アドレスバスが 16 ビットの場合、PROM セルを 512 バイト単位に指定できるが、前記アドレスレジスタ 14-21 のビット長を変更することにより、任意の容量のメモリ領域をコンフィデンシャル・ゾーン

として指定できる。以上アドレスレジスタ14-21にデータを設定することにより、コンフィデンシャル・ゾーン11-2のアドレス値が確定し、以後コンフィデンシャル・ゾーン11-2へのデータ書き込みが禁止される。

次にアドレスレジスタ14-21にデータを設定し、書き込み禁止フラグ14-2をセットした後、コンフィデンシャル・ゾーン11-2への書き込みが実行されたとする。比較器14-20はアドレスバス3上のコンフィデンシャル・ゾーンのアドレス領域とアドレスレジスタ14-21内のコンフィデンシャル・ゾーンのアドレスデータの一致を検出し、その一致信号をコンフィデンシャル・ゾーン選択線14-7に出力してコンフィデンシャル・ゾーン11-2が選択されたことを通知する。しかし書き込み禁止フラグ14-2がセットされていることにより書き込み禁止線14-6はハイレベルであるので、第1のアンドゲート14-8、第2のアンドゲート14-12によりライト信号線15がアクティブになっても、コンフィデンシ

ャル・ゾーンライトストロブ線14-10はハイレベルとならず、コンフィデンシャル・ゾーンへのデータ書き込みは行なうことができない。さらに第1のアンドゲートの出力14-9がハイレベルで(書き込み禁止中にコンフィデンシャル・ゾーンが選択された時)ライト信号線15がハイレベルになると、第3のアンドゲート14-13によりアクセスエラー割込み信号14-11を発生し、プロセッサにアクセスエラーの割込み処理を実行させる。

よって上述のように、本第2の実施例においては半固定のアドレスレジスタ(書き込み禁止フラグを含む)及び比較器を付加することにより、コンフィデンシャル・ゾーン11-2の領域の指定を行なうことができる。さらに前記アドレスレジスタは半固定であるため、前記コンフィデンシャル・ゾーン領域指定後の前記領域の変更及びコンフィデンシャル・ゾーン内のデータの不当な書き換えやプログラムの暴走によるコンフィデンシャル・ゾーン内のデータの破壊を防止することができ、

コンフィデンシャル・ゾーンのフェイル・セーフが完全となる。

次にコンフィデンシャル・ゾーン内のデータ読み出しについてであるが、これも前記従来例と同様に行ない、不正なアクセスに対する対処はソフトウェア処理により行なう。

〔発明の効果〕

以上説明したように本発明においては、従来データメモリとして使用しているPROMブロックに対し、書き込み禁止フラグやPROMメモリ中のコンフィデンシャル・ゾーンに対するアドレスデコードまたはアドレスレジスタ、比較器など簡単なハードウェアを付加することにより、従来コンフィデンシャル・ゾーンへのデータ書き込み禁止をソフトウェア処理により行なっていた時に生じる不当なデータ書き込みに対してセキュリティ性をより高める効果がある。

またROM内のプログラムが暴走した場合でも、コンフィデンシャル・ゾーン内のデータは前記ハードウェアにより完全に保護されるため、より確

実なフェイル・セーフが実現できる効果がある。

#### 4. 図面の簡単な説明

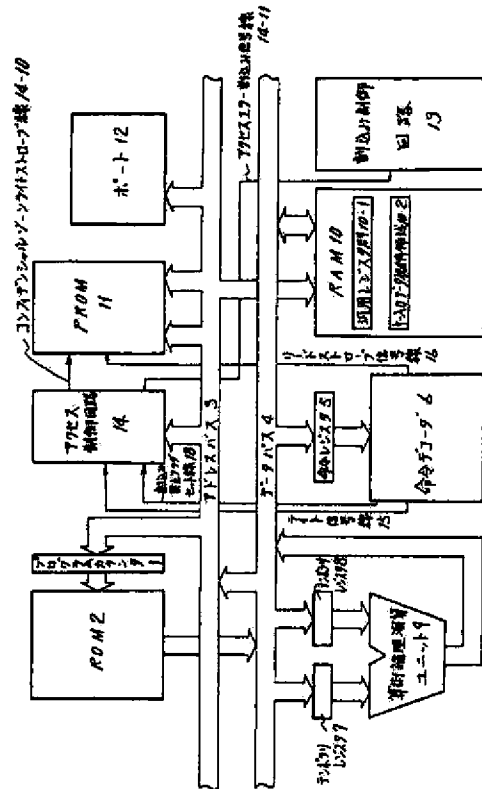
第1図は本発明の第1及び第2の実施例におけるシングルチップマイクロコンピュータのブロック図、第2図は第1図における第1の実施例のアクセス制御回路及びPROMの詳細図、第3図は第1図における第2の実施例のアクセス制御回路及びPROMの詳細図、第4図は本発明における書き込み禁止フラグの回路構成図、第5図は従来のシングルチップマイクロコンピュータのブロック図、第6図は従来のコンフィデンシャル・ゾーンアクセスのフローチャートである。

1……プログラムカウンタ、2……ROM、3……アドレスバス、4……データバス、5……命令レジスタ、6……命令デコード、7……テンポラリレジスタ、8……テンポラリレジスタ、9……算術論理演算ユニット、10……RAM、10-1……汎用レジスタ群、10-2……キー入力データ格納領域、10-3……読み出し許可フラ

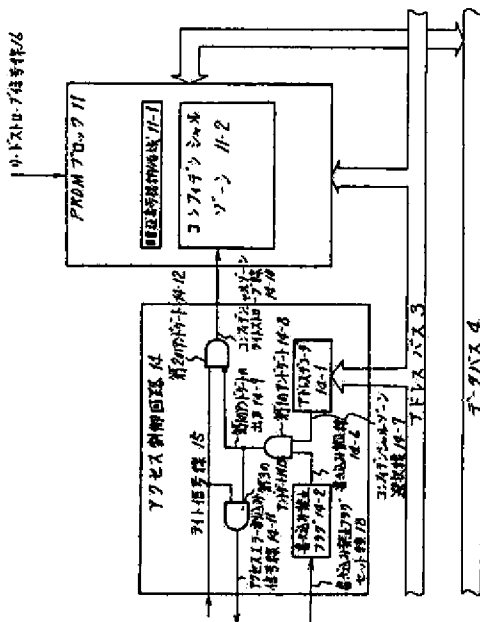


グ、11……PROM、11-1……寄証番号格納領域、11-2……コンフィデンシャル・ゾーン、11-3……書き込み禁止フラグ、12……ポート、13……割込み制御回路、14……アクセス制御回路、14-1……アドレスデコーダ、14-2……書き込み禁止フラグ、14-6……書き込み禁止線、14-7……コンフィデンシャル・ゾーン選択線、14-8……第1のアンドゲート、14-9……第1のアンドゲートの出力、14-10……コンフィデンシャル・ゾーンライトストロブ線、14-11……アクセスエラー割込み信号線、14-12……第2のアンドゲート、14-13……第3のアンドゲート、14-20……比較器、14-21……アドレスレジスタ、15……ライト信号線、16……リードストロブ信号線、18……書き込み禁止フラグセット線、19……nチャネルトランジスタ、20……抵抗、21……ヒューズ抵抗。

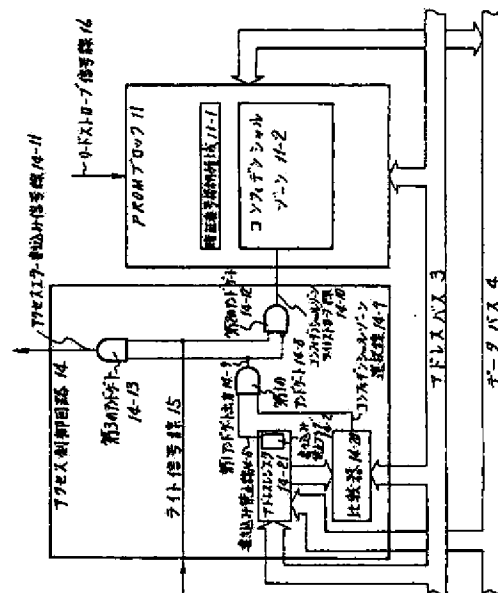
代理人 井理士 内 原 資



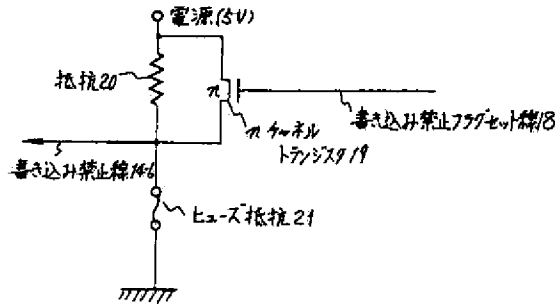
第 1 図



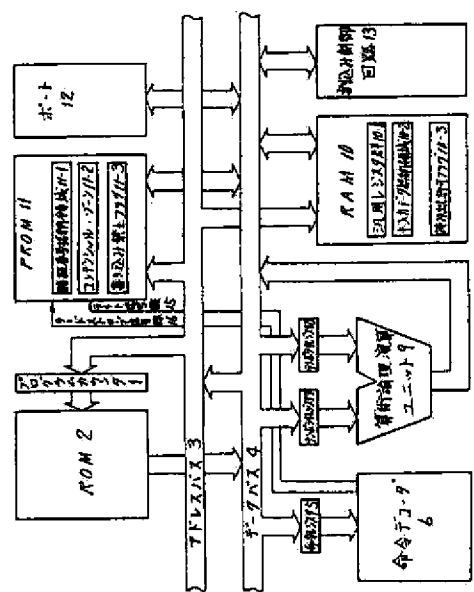
第 2 図



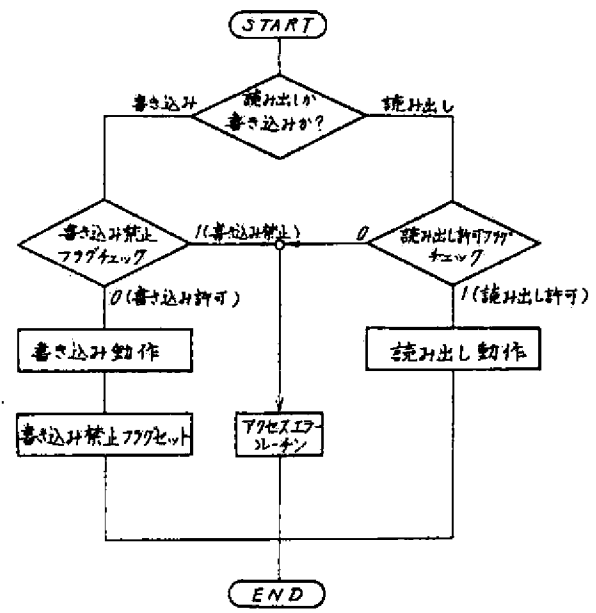
第 3 図



第 4 図



第 5 図 (従来例)



第 6 図 (従来例)